(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2002064482 A

(43) Date of publication of application: 28.02.02

(51) Int. Cl H04L 9/14

(21) Application number: 2000252787

(22) Date of filing: 23.08.00

(71) Applicant: MATSUSHITA ELECTRIC WORKS LTD

(72) Inventor: MIURA TOSHIBUMI

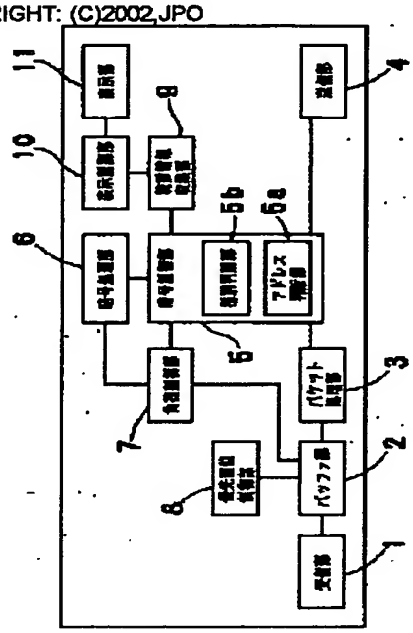
# (54) ENCRYPTION APPARATUS



(57) Abstract:

PROBLEM TO BE SOLVED: To provide an encryption apparatus for reducing the amount of scrap of received data and preventing the capacity of the whole network from being reduced.

SOLUTION: The encryption apparatus comprises a receiving section 1 for receiving data from the outside, a transmitting section 2 for transmitting the data to the outside, an encryption control section 5 for making a judgment whether the encrypting of the data received from the receiving section is necessary or not based on the address from which the data is transmitted or the address to which the data is transmitted, an encryption section 6 for encrypting the data, which the encryption section 5 judges to be encrypted, by the use of one encryption mode of a plurality of encryption modes and for outputting the encrypted data to the transmitting section 2, and a load control section 7 for monitoring the encrypting load of the encryption section 6 and changing the encryption mode of the encryption section 6 according to the encrypting load.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－64482
（P2002－64482A）
(43)公開日　平成14年２月28日(2002.2.28)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｈ０４Ｌ　9/14 | | Ｈ０４Ｌ　9/00 | ６４１ | ５Ｊ１０４ |

審査請求　未請求　請求項の数12　ＯＬ　（全９頁）

(21)出願番号　特願2000－252787(P2000－252787)

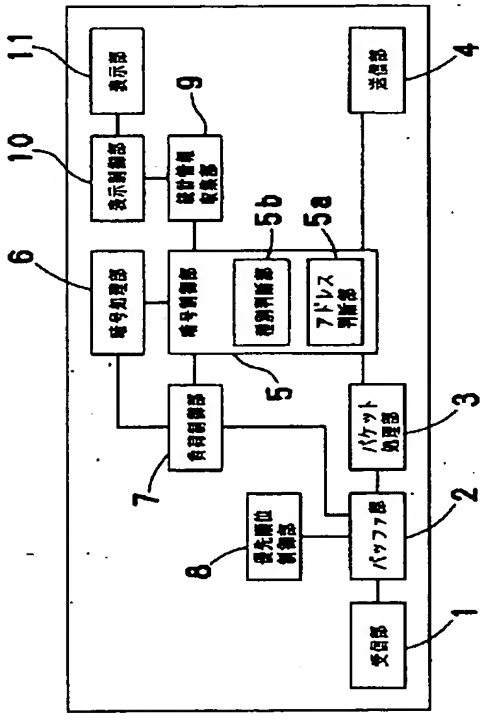
(22)出願日　平成12年８月23日(2000.8.23)

(71)出願人　000005832
松下電工株式会社
大阪府門真市大字門真1048番地
(72)発明者　三浦　俊文
大阪府門真市大字門真1048番地松下電工株式会社内
(74)代理人　100111556
弁理士　安藤　淳二　（外１名）

Ｆターム(参考)　5J104 AA33 AA35 AA36

(54)【発明の名称】　暗号処理装置

(57)【要約】
【課題】　受信するデータの破棄を低減し、ネットワーク全体の性能の低減を防止する暗号処理装置等を提供する。
【解決手段】　外部からデータを受信する受信部１と、外部にデータを送信する送信部２と、受信部から受け取ったデータの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断する暗号制御部５と、暗号制御部が暗号処理を要すると判断したデータを、複数の備えた暗号方式の内の一つの暗号方式により暗号処理し処理結果のデータを送信部に出力する暗号処理部６と、を備えた暗号処理装置において、暗号処理部の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更する負荷制御部７を備えて構成した。



1

【特許請求の範囲】

【請求項１】　外部からデータを受信する受信部と、外部にデータを送信する送信部と、受信部から受け取ったデータの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断する暗号制御部と、該暗号制御部が暗号処理を要すると判断したデータを、複数の備えた暗号方式の内の一つの暗号方式により暗号処理し処理結果のデータを送信部に出力する暗号処理部と、を備えた暗号処理装置において、

暗号処理部の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更する負荷制御部を備えたことを特徴とする暗号処理装置。

【請求項２】　前記負荷制御部は、暗号処理部における暗号処理の負荷が高負荷である場合に、暗号処理部の暗号方式をより負荷の軽い暗号方式に変更することを特徴とする請求項１記載の暗号処理装置。

【請求項３】　前記暗号制御部に、データの種別を判別し、該種別によって暗号処理の要否を判断する種別判断部を設け、該種別判断部は暗号処理を要すると判断したデータを暗号処理部に出力することを特徴とする請求項１又は請求項２記載の暗号処理装置。

【請求項４】　前記暗号処理部は、前記種別判断部の判別しする種別に応じた暗号方式で暗号処理することを特徴とする請求項３記載の暗号処理装置。

【請求項５】　前記受信部と暗号制御部との間に、受信したデータを一時的に蓄積記憶するバッファ部と、該バッファ部内に蓄積記憶されているデータに優先順位を付する優先順位制御部とを設け、暗号制御部は、前記優先順位の高いデータから暗号処理の要否を判断することを特徴とする請求項１乃至請求項４のいずれかに記載の暗号処理装置。

【請求項６】　前記暗号処理部の暗号処理に用いる暗号方式を表示する表示部を設けたことを特徴とする請求項１乃至請求項５記載の暗号処理装置。

【請求項７】　外部からデータを受信するステップと、受信部から受け取ったデータの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断するステップと、該暗号制御部が暗号処理を要すると判断したデータを、複数の備えた暗号方式の内の一つの暗号方式により暗号処理するステップと、処理結果のデータを送信するステップと、を備えた暗号処理方法において、

暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更するステップを備えたことを特徴とする暗号処理方法。

【請求項８】　前記負荷を監視して暗号方式を変更するステップは、暗号処理の負荷が高負荷である場合に、暗号方式をより負荷の軽い暗号方式に変更することを特徴とする請求項７記載の暗号処理方法。

【請求項９】　前記暗号処理の要否を判断するステップに、データの種別を判別し、該種別によって暗号処理の要否を判断するステップを設けたことを特徴とする請求項７又は請求項８記載の暗号処理方法。

【請求項１０】　前記暗号処理するステップは、前記判別した種別に応じた暗号方式で暗号処理することを特徴とする請求項９記載の暗号処理方法。

【請求項１１】データを受信するステップの後に、受信したデータを一時的に蓄積記憶するステップと、該蓄積記憶されているデータに優先順位を付するステップとを設け、前記暗号処理の要否を判断するステップは、前記優先順位の高いデータから暗号処理の要否を判断することを特徴とする請求項７乃至請求項１０のいずれかに記載の暗号処理方法。

【請求項１２】　前記請求項６乃至請求項１１のいずれかに記載の暗号処理方法を実行するためのプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、一方側から受信したデータを暗号処理して他方側へ送信する暗号処理装置に関する。

【０００２】

【従来の技術】近年、データ通信のセキュリティを目的として、コンピュータ端末近傍に暗号処理装置を配して、当該コンピュータ端末から送信されるデータには暗号化処理を施して暗号データを送信し、コンピュータ端末側に受信される暗号データには復号化処理を施して通常のデータとして受信する場合がある。このような場合に用いられる暗号処理装置にあっては、データの送信元アドレスや送信先アドレスなどによって暗号処理をデータに施すか否かを判断して、必要なものだけを暗号処理して送受信するということが行われている。

【０００３】

【発明が解決しようとする課題】しかしながら、従来の暗号処理装置にあっては、暗号処理に複雑な計算を要するため暗号処理の負荷が大きくなり、次々と受信するデータの処理が間に合わない場合があった。このように先に受信されたデータの暗号処理が終わる前に次のデータが受信された場合、後続のデータは破棄され、データの送信元は再度ネットワーク上にデータを送信しなければならなかった。また、これに対処すべくバッファを設け、該バッファにデータを蓄積して順次処理するものもあるが、次々にデータを受信した場合には処理が間に合わないとバッファが溢れてしまい、溢れたデータは破棄され、再度データの送信が行われることとなる。その結果、暗号処理装置を一つのノードとするネットワーク全体の性能を低減させる恐れがあるという問題点があった。

【０００４】本発明は、上記問題点を改善するために成されたもので、その目的とするところは、受信するデー

タの破棄を低減し、ネットワーク全体の性能の低減を防止する暗号処理装置、暗号処理方法及びその方法を実行するプログラムを記録した記録媒体を提供することにある。

【０００５】

【課題を解決するための手段】上記の問題を解決するために、本発明の暗号処理装置にあっては、外部からデータを受信する受信部と、外部にデータを送信する送信部と、受信部から受け取ったデータの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断する暗号制御部と、該暗号制御部が暗号処理を要すると判断したデータを、複数の備えた暗号方式の内の一つの暗号方式により暗号処理し処理結果のデータを送信部に出力する暗号処理部と、を備えた暗号処理装置において、暗号処理部の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更する負荷制御部を備えたことを特徴とするものである。

【０００６】前記負荷制御部は、暗号処理部における暗号処理の負荷が高負荷である場合に、暗号処理部の暗号方式をより負荷の軽い暗号方式に変更するものであることが好ましい。ここで、高負荷とは、これ以上そのままの処理を継続すると、送信するデータよりも受信するデータが多くなって、全てのデータを処理することができず、受信するデータの一部又は全部を破棄する恐れのあるような場合をいう。

【０００７】また、暗号制御部に、データの種別を判別し、該種別によって暗号処理の要否を判断する種別判断部を設け、該種別判断部は暗号処理を要すると判断したデータを暗号処理部に出力するようにしてもよい。種別とは、データが適用されるアプリケーションソフトウェアや、データのタイプなど、データ自体の特徴を表す属性をいう。そして、この場合には、種別判断部は、種別に応じた暗号方式で暗号処理することを暗号処理部に指示することがより好ましい。

【０００８】一方、前記受信部と暗号制御部との間に、受信したデータを一時的に蓄積記憶するバッファ部と、該バッファ部内に蓄積記憶されているデータに優先順位を付する優先順位制御部とを設け、暗号制御部は、前記優先順位の高いデータから暗号処理の要否を判断するものであってもよい。

【０００９】更に、暗号処理部の暗号処理に用いる暗号方式を表示する表示部を設けるようにしてもよい。また、表示部は暗号方式以外の暗号処理に関する情報を表示するものであってもよい。

【００１０】また、本発明の暗号処理方法にあっては、暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更するステップを備えたことを特徴とするものである。また、負荷を制御し暗号方式を変更するステップは、暗号処理の負荷が高負荷である場合に、暗号方式をより負荷の軽い暗号方式に変更することを特



徴とするものが好ましい。

【００１１】記暗号処理の要否を判断するステップに、データの種別を判別し、該種別によって暗号処理の要否を判断するステップを設ることも好ましく、この場合、暗号処理するステップは、前記判別した種別に応じた暗号方式で暗号処理するようにすればより好ましい。

【００１２】一方、データを受信するステップの後に、受信したデータを一時的に蓄積記憶するステップと、該蓄積記憶されているデータに優先順位を付するステップとを設け、暗号処理の要否を判断するステップは、前記優先順位の高いデータから暗号処理の要否を判断するものであってもよい。

【００１３】また、本発明の記録媒体にあっては、上記の暗号処理方法を実行するためのプログラムを記録したことを特徴とするものである。

【００１４】

【発明の実施の形態】本発明にかかる暗号処理装置の第一実施の形態を図１乃至図５基づいて説明する。図１は本発明の暗号処理装置の一構成例を示すブロック図であり、図２は暗号処理装置の外観を示す斜視図である。図３は本発明の暗号処理装置の全体の動作を説明するフローチャートである。図４は本発明の暗号処理装置の暗号方式の変更動作の他の例を説明するフローチャートである。

【００１５】図１において、暗号処理装置は、受信部１、バッファ部２、パケット処理部３、送信部４、暗号制御部５、暗号処理部６、負荷制御部７、優先順位制御部８、統計情報収集部９、表示制御部１０、表示部１１を備えて構成されており、特定送信元アドレスからのデータ又は特定宛先アドレスへのデータについて通過させるとともに、更にその中で特定の送信元アドレスからのデータ又は特定宛先アドレスへのデータについてはデータを暗号化して送信させるものである。従って、データには暗号処理装置を通過できないもの、暗号処理装置をそのまま暗号化されずに通過するもの、及び暗号処理装置にて暗号化されて通過するもの、の３種類がある。

【００１６】受信部１は、コネクタを有しており該コネクタに接続された信号線を介して外部からのデータを受信するものである。受信されるデータは、暗号化処理がなされておらずそのままで内容の把握が可能な平文データであり、例えばパケットの形式をとっている。受信部１は、データを受信すると、該データをバッファ部２に出力する。

【００１７】バッファ部２は、受信したデータを一時的に蓄積記憶するものであり、読み書き可能なメモリで構成されている。バッファ部２は、データを受け取ると、待ち行列の最後尾にデータを格納する。バッファ部２を設けることにより、前のデータの暗号処理が終了するまでに次のデータを受信しても、該次のデータを蓄積記憶できるため、データの破棄を防止することができる。

【００１８】パケット処理部３は、バッファ部２の待ち行列の先頭からデータを取り出して、暗号処理装置を通過させて良いか否かを判断するものである。パケット処理部３は、バッファ部２の暗号処理装置の通過を許可する特定の送信元アドレスからのデータ又は特定宛先アドレスへのデータについては暗号制御部５に出力し、暗号処理装置の通過を許可しない他のデータについてはデータを破棄する。なお、データの送信元アドレス又は宛先アドレスと、通過の要否との関係は、別途設定テーブルを設けておいて、パケット処理部３は該テーブルを参照して判断するようになしてある。

【００１９】暗号制御部５は、暗号処理装置を通過させるデータについて、暗号処理を行うか否かを判断するものであり、アドレス判断部５ａと、種別判断部５ｂとを備えている。

【００２０】アドレス判断部５ａは、データの送信元アドレス又は宛先アドレスに基づいて該データの暗号処理の要否を判断するものであり、暗号処理を必要としないデータについてはそのまま送信部４に出力し、暗号処理が必要なデータについては種別判断部５ｂに出力する。なお、データの送信元アドレス又は宛先アドレスと、暗号処理の要否との関係は、別途設定テーブルを設けておいて、アドレス判断部５ａは該テーブルを参照して判断するようになしてある。

【００２１】種別判断部５ｂは、データの種別を判別し、該種別によって暗号処理の要否を判断するものである。種別とは、特定のワードプロセッサーや特定の画像処理ソフトウェア等のようにデータが対応するアプリケーションソフトウェアの種類であってもよいし、テキストデータ、イメージデータなどのデータのタイプであってもよい。本実施の形態では、データが対応するアプリケーションソフトウェアの種類を種別として用いている。種別判断部５ｂは、データの種別に基づいて暗号処理を必要としないと判断したデータについてはそのまま送信部４に出力し、データの種別に基づいて暗号処理が必要と判断したデータについては暗号処理部６に出力する。その際、種別判断部５ｂは、種別に応じた暗号方式で暗号処理することを暗号処理部に指示するようになしてある。具体的には、種別判断部５ｂは、例えばアプリケーションソフトウェアＰに対応するデータについては、暗号方式Ｘにて暗号処理を行うように指示し、アプリケーションソフトウェアＱに対応するデータについては、暗号方式Ｙにて暗号処理を行うように指示する。なお、種別と、暗号処理の要否及び暗号方式との関係は、別途設定テーブルを設けておいて、種別判断部５ｂは該テーブルを参照して判断するようになしてある。

【００２２】種別判断部５ｂにより、データの種別により暗号処理の要否判断を行うことにより、データの種別によっては暗号処理が不要となる場合に、該不要な暗号処理を行うことがなく、よって暗号処理動作の負荷を軽減することができる。つまり、アドレス判断部５ａにて暗号処理を要すると一律に判断されたデータの中でも、データの種別によっては暗号処理をする必要のないものが存在する場合があり、これらデータの暗号処理を省くことにより暗号処理動作の負荷を軽減することが可能となる。また、種別判断部５ｂは、種別に応じた暗号方式で暗号処理することを暗号処理部に指示するため、種別に応じた暗号強度を選択することが可能となり、一律の暗号強度とする場合に比べて暗号処理の効率を高めることが可能となる。



【００２３】暗号処理部６は、例えばシングルＤＥＳ方式やトリプルＤＥＳ方式等の複数の暗号方式による暗号処理が可能であって、暗号制御部５から受け取ったデータを、種別判断部５ｂの指定する暗号方式により暗号化するものである。但し、暗号処理部６は次に説明する負荷制御部７からも暗号方式を指定される場合があり、負荷制御部７から指定があった場合には、その指定に優先して従うようになしてある。暗号処理部６は、暗号処理されたデータを暗号制御部５を介して送信部４に出力する。

【００２４】負荷制御部７は、暗号処理部６の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部６の暗号方式を変更するものである。負荷制御部７は、暗号処理動作の負荷が所定の負荷閾値Ａ以上の場合である高負荷の場合には、暗号方式をより負荷の軽い他の暗号方式に変更するよう暗号処理部６に指示をする。負荷閾値は、暗号処理部６にかかる負荷を表す値であれば良いが、本実施の形態ではバッファ部２に蓄積される未処理のデータ個数としている。

【００２５】具体的には、負荷制御部７は、バッファ部２の待ち行列に入っているデータの個数を検出して、バッファ部２の待ち行列からデータが溢れそうな程度にデータが蓄積記憶されている場合に、暗号処理動作が高負荷であると判断する。例えば、負荷制御部７は、バッファ部２の待ち行列の８割にデータが記憶された場合に、負荷閾値Ａ以上であり高負荷と判断する。そして、負荷制御部７は、暗号処理動作が高負荷であると判断した場合には、暗号処理部６の暗号方式をより負荷の軽い暗号方式に変更するよう、暗号処理部６に指示を出す。例えば、暗号制御部７は、暗号処理部６が暗号方式Ｙで暗号処理を行おうとしている場合に、より負荷の軽い暗号方式Ｘへの変更を指示する。

【００２６】優先順位制御部８は、バッファ部２内に蓄積記憶されているデータに優先順位を付するものであり、優先順位の高いデータが待ち行列の先頭となるようにデータを制御するものである。この場合、優先順位制御部８は、待ち行列に入るデータを記憶し直してメモリの中で物理的にデータが優先順位の順番に並ぶようにしてもよいし、データに優先順位を示すインデックスを別途設けておいて、論理的に優先順位の順番にならぶよう

にして、パケット処理部３がインデックスに示された優先順位順にデータを取り出すようにしてもよい。優先順位制御部８は、データのプロトコル、対応アプリケーションソフトウェア、ファイルタイプ、宛先アドレス、送信元アドレス等に基づいて優先順位を決定する。

【００２７】統計情報収集部９は、暗号処理部６の処理する暗号方式について、各暗号方式の使用回数、暗号方式の変更回数等の各種の統計情報、及び現在処理中の暗号方式を収集するものである。

【００２８】表示制御部１０は、統計情報収集部９の収集した統計情報及び現在処理中の暗号方式を表示部１１に出力するものである。具体的には、表示制御部１０は、図２に示すように、統計情報を表示部１１の液晶表示部１１ａに出力して文字や図形情報として視覚化し、現在処理中の暗号方式については表示部１１のＬＥＤ表示部１１ｂに出力する。ＬＥＤ表示部１１ｂは複数のＬＥＤを備えており、点灯パターンにより暗号方式を示すようになしてある。

【００２９】次に以上のようにして構成した暗号処理装置の動作を図３を用いて説明する。

【００３０】まず、受信部１がデータをパケット形式で受信して（ステップＳ１０１）、該受信データをバッファ部２に蓄積記憶する。その際に、優先順位制御部８が該蓄積記憶されているデータに優先順位を付与する（ステップＳ１０１）。そして、パケット処理部３が、バッファ部２の待ち行列の中から優先順位の最も高いデータを取り出して、送信元アドレス、宛先アドレスに基づいて、データを通過させてよいか否かを判断する（ステップＳ１０２）。

【００３１】パケット処理部３は、データを通過させてもよいと判断した場合には、該データを暗号制御部５に出力する。暗号制御部５では、まずアドレス判断部５ａがデータの送信元アドレス、宛先アドレスから暗号処理の要否を判断し（ステップＳ１０３）、暗号処理不要と判断されたデータはそのまま送信される（ステップＳ１１２）。一方、暗号処理が必要と判断されたデータは、種別判断部５ｂに出力され、更にデータの種別に基づいて、暗号処理の要否が判断される（ステップＳ１０４）。具体的には、本実施の形態では、データに対応するアプリケーションソフトウェアに基づいて暗号処理の要否を判断するようにしてある。そして、暗号処理不要と判断されたデータはそのまま送信され（ステップＳ１１２）、暗号処理が必要と判断されたデータは暗号処理部６に出力されるとともに、種別判断部５ｂは暗号方式を指定して暗号処理部６に指示を行う（ステップＳ１０５～Ｓ１０７）。

【００３２】次に負荷制御部７は、現在の暗号処理部６における暗号処理の負荷を監視し、現在の暗号方式を確認した上で（ステップＳ１０８）、暗号方式として処理負荷の高い暗号方式Ｙが指定されており、暗号処理動作の負荷が所定の負荷閾値Ａ以上の場合である高負荷の場合には（ステップＳ１０９）、暗号方式Ｙをより負荷の軽い暗号方式Ｘに変更するよう暗号処理部６に指示をし（ステップＳ１１０）、暗号処理動作の負荷が所定の負荷閾値Ａ未満の場合であるには暗号方式の変更は行わない。また、暗号方式として負荷の軽い暗号方式Ｘが指定されている場合にも、暗号方式を変更することなく処理を続行する（ステップＳ１０８）。

【００３３】以上のようにして指定された暗号方式に基づいて、暗号処理部６はデータを暗号化し（ステップＳ１１１）、該暗号化したデータを暗号制御部５を介して送信部４に出力する。送信部４は該データを外部に送信し（ステップＳ１１２）、一連の動作が完了する。該動作は繰り返し行われる。但し、ステップＳ１０２～ステップＳ１１２までの一連の流れは連続して１ステップづつ行われるが、データの受信処理（ステップＳ１０１）は上記一連の流れとは別個に行われる。

【００３４】なお、上記説明では、暗号処理動作の負荷が軽い場合には特に暗号方式を変更することはしていないが、図４に示すように、より負荷の高い暗号方式に変更する（ステップＳ１１３，Ｓ１１４）ようにしてもよい。この場合、暗号処理装置の負荷が軽い場合にはより強度の暗号化を行ったデータを送信することができるという利点がある。

【００３５】以上のようにして構成した暗号処理装置及び暗号処理方法にあっては、負荷が高くなりバッファ部２からデータが溢れそうになった場合に、暗号処理部６での暗号方式を負荷の軽いものに変更するので、データ溢れを防止して、データが破棄されることを防ぐことができ、ひいては暗号処理装置を一つのノードとするネットワーク全体の性能の低下を防止することができる。

【００３６】なお、本発明の暗号処理装置は、上述したもののみ限定されるものではなく、本発明の要旨を逸脱しない範囲内において種々変更を加え得ることは勿論である。

【００３７】

【発明の効果】本発明の御号処理装置は上述のように構成してあるから、請求項１記載の発明にあっては、負荷制御部が、暗号処理部の暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更するので、負荷状況に対応した暗号方式を用いることができるという効果を奏する。

【００３８】請求項２記載の発明にあっては、負荷制御部は、暗号処理部における暗号処理の負荷が高負荷である場合に、暗号処理部の暗号方式をより負荷の軽い暗号方式に変更するので、暗号処理動作の過負荷によるデータの破棄を防止し、ネットワーク全体の性能の低下を防止することができるという効果を奏する。

【００３９】請求項３記載の発明にあっては、暗号制御部に、データの種別を判別し、該種別によって暗号処理

の要否を判断する種別判断部を設け、該種別判断部は暗号処理を要すると判断したデータを暗号処理部に出力するので、データの種別によっては暗号処理が不要となる場合に、該不要な暗号処理を行うことがなく、よって暗号処理動作の負荷を軽減することができるという効果を奏する。

【００４０】請求項４記載の発明にあっては、暗号処理部が、種別判断部の判別する種別に応じた暗号方式で暗号処理するので、データの種別毎に暗号強度を適宜設定でき、効率的に暗号処理をすることにより、暗号処理動作の負荷を軽減することができるという効果を奏する。

【００４１】請求項５記載の発明にあっては、優先順位制御部が、バッファ部内に蓄積記憶されているデータに優先順位を付け、暗号制御部は、優先順位の高いデータから暗号処理の要否を判断するので、優先順位の高いデータをより素早く処理して送信することができるという効果を奏する。

【００４２】請求項６記載の発明にあっては、表示部が暗号処理部の暗号処理に用いる暗号方式を表示するので、使用者は現在の暗号方式を目視確認することができ、暗号処理装置の誤動作の確認をすることが容易になるという効果を奏する。

【００４３】請求項７記載の発明にあっては、暗号処理動作の負荷を監視し、該負荷に応じて暗号処理部の暗号方式を変更するステップを備えたので、負荷状況に対応した暗号方式を用いることができるという効果を奏する。

【００４４】請求項８記載の発明にあっては、負荷を制御し暗号方式を変更するステップは、暗号処理の負荷が高負荷である場合に、暗号方式をより負荷の軽い暗号方式に変更するので、暗号処理動作の過負荷によるデータの破棄を防止し、ネットワーク全体の性能の低下を防止することができるという効果を奏する。

【００４５】請求項９記載の発明にあっては、暗号処理の要否を判断するステップに、データの種別を判別し、該種別によって暗号処理の要否を判断するステップを設けたので、データの種別によっては暗号処理が不要となる場合に、該不要な暗号処理を行うことがなく、よって



暗号処理動作の負荷を軽減することができるという効果を奏する。

【００４６】請求項１０記載の発明にあっては、暗号処理するステップは、判別した種別に応じた暗号方式で暗号処理するので、データの種別毎に暗号強度を適宜設定でき、効率的に暗号処理をすることにより、暗号処理動作の負荷を軽減することができるという効果を奏する。

【００４７】請求項１１記載の発明にあっては、データを受信するステップの後に、受信したデータを一時的に蓄積記憶するステップと、該蓄積記憶されているデータに優先順位を付するステップとを設け、暗号処理の要否を判断するステップは、前記優先順位の高いデータから暗号処理の要否を判断するので、優先順位の高いデータをより素早く処理して送信することができるという効果を奏する。

【００４８】請求項１２記載の発明にあっては、記録媒体をコンピュータ等に読み込み実行させることにより、請求項７乃至請求項１１のいずれかに記載の発明の効果を奏する。

【図面の簡単な説明】

【図１】本発明の暗号処理装置の構成の一例を示すブロック図である。

【図２】本発明の暗号処理装置の外観を示す斜視図である。

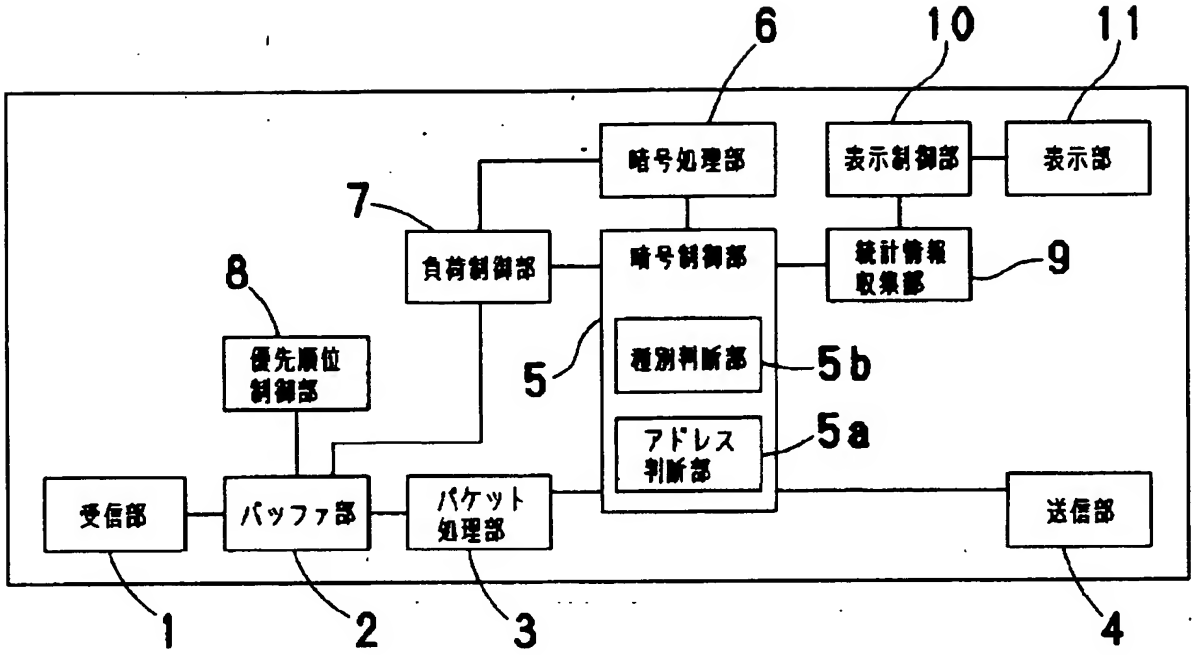
【図３】本発明の暗号処理方法の一例を示すフローチャートである。

【図４】本発明の暗号処理方法の他の例を示すフローチャートである。

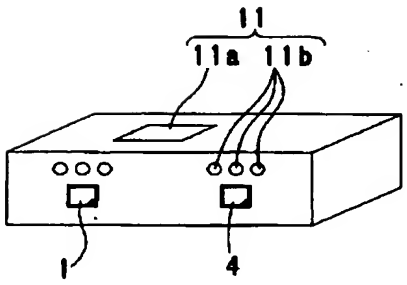
【符号の説明】

１　受信部
２　バッファ部
４　送信部
５　暗号制御部
５ｂ　種別判断部
６　暗号処理部
７　負荷制御部
８　優先順位制御部
１１　表示部

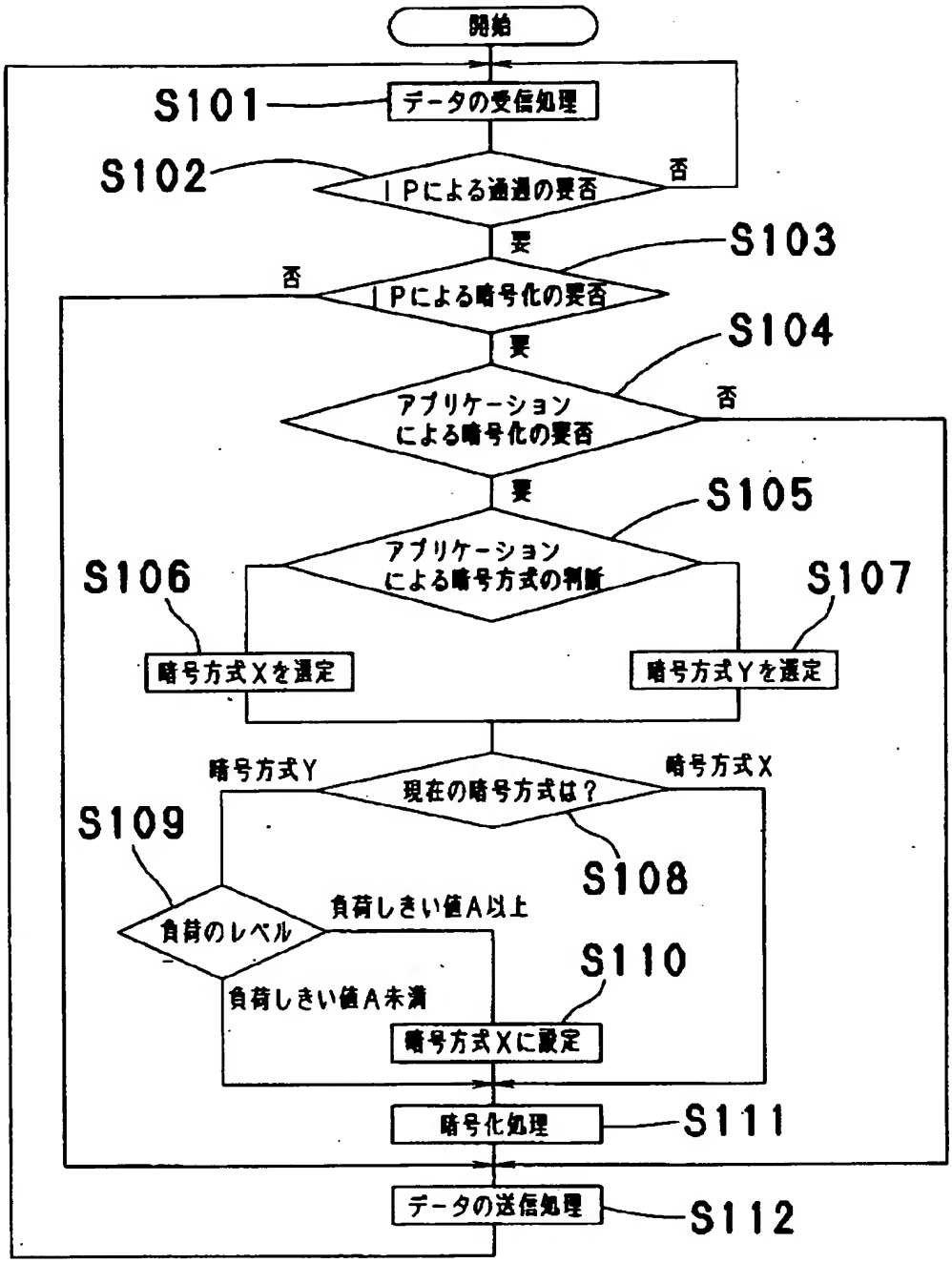
【図１】


6
10
11
暗号処理部
表示制御部
表示部
7
負荷制御部
暗号制御部
統計情報収集部
9
8
優先順位制御部
5
種別判断部
5b
アドレス判断部
5a
受信部
バッファ部
パケット処理部
送信部
1
2
3
4

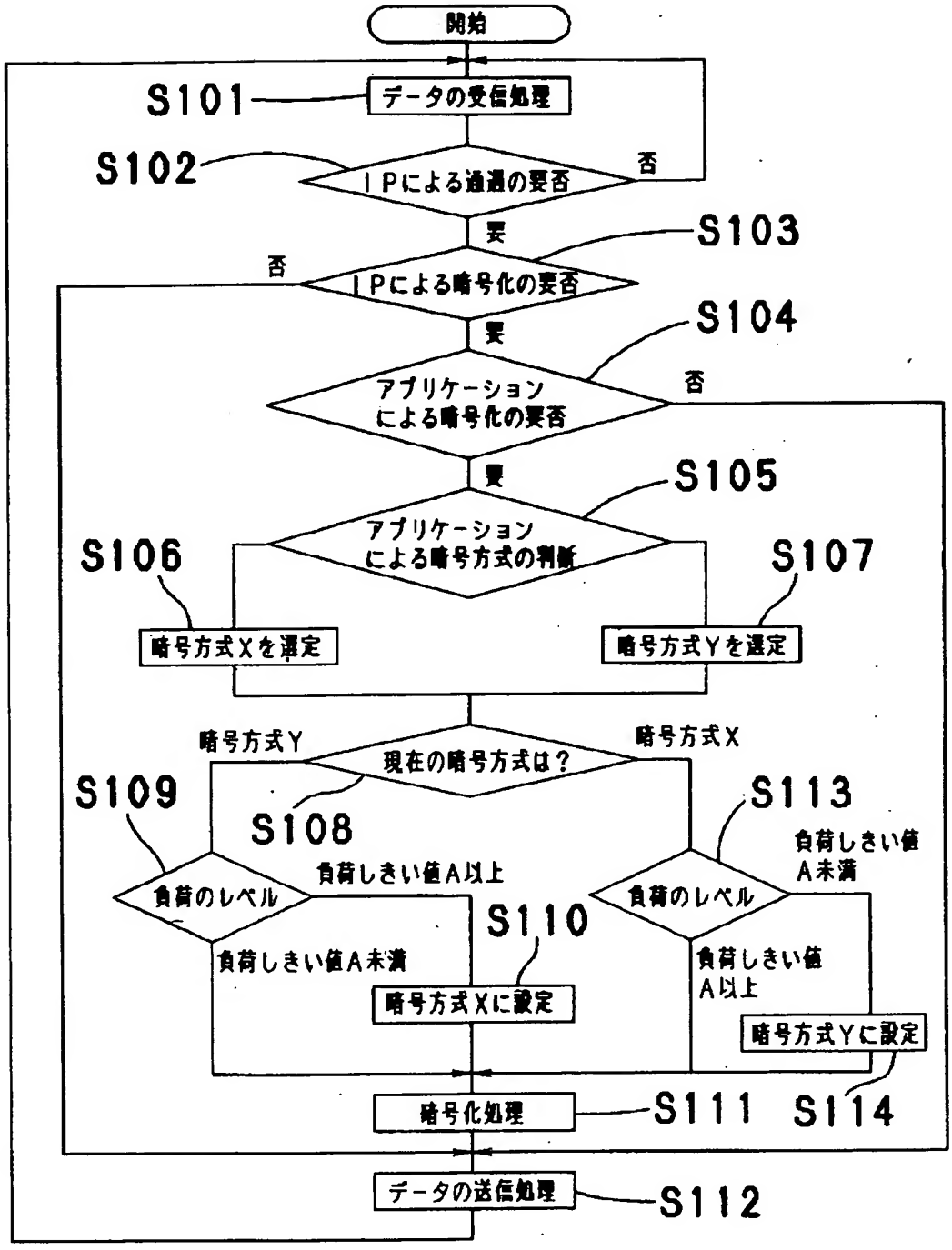
【図２】


11
11a
11b
1
4

【図３】


開始
S101
データの受信処理
S102
IPによる通過の要否
否
要
S103
IPによる暗号化の要否
否
要
S104
アプリケーション
による暗号化の要否
否
要
S105
アプリケーション
による暗号方式の判断
S106
S107
暗号方式Xを選定
暗号方式Yを選定
暗号方式Y
現在の暗号方式は？
暗号方式X
S109
S108
負荷のレベル
負荷しきい値A以上
S110
負荷しきい値A未満
暗号方式Xに設定
暗号化処理
S111
データの送信処理
S112

【図４】


開始
S101
データの受信処理
S102
IPによる通過の要否
否
要
S103
IPによる暗号化の要否
否
要
S104
アプリケーション
による暗号化の要否
否
要
S105
アプリケーション
による暗号方式の判断
S106
S107
暗号方式Xを選定
暗号方式Yを選定
暗号方式Y
現在の暗号方式は？
暗号方式X
S109
S108
S113
負荷しきい値A以上
負荷のレベル
負荷しきい値
A未満
負荷のレベル
S110
負荷しきい値A未満
負荷しきい値
A以上
暗号方式Xに設定
暗号方式Yに設定
暗号化処理
S111
S114
データの送信処理
S112